

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-314014

(43)Date of publication of application : 26.11.1993

(51)Int.Cl. G06F 12/14
G06F 3/06
G06F 9/06

(21)Application number : 04-114864

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 07.05.1992

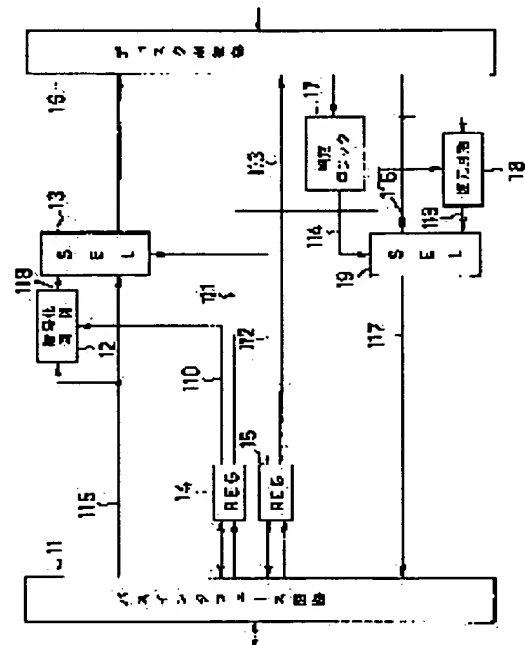
(72)Inventor : KUWABARA KAZUYOSHI

(54) DISK CONTROLLER

(57)Abstract:

PURPOSE: To incorporate hardware for enciphering and deciphering data into a disk controller.

CONSTITUTION: The data to show whether the data generated by an external device is to be enciphered and written or not is set in a register 14, and an encipherment key is set in the register 15, and at the time of writing the data to a disk device, by referring to contents set in each register 14, 15, raw write data or write data having passed through an encipherment circuit 12 is outputted to a disk control apt 16 together with attribute information to show whether it is enciphered or not, and at the time of read, whether read data is enciphered or not is judged by judgement logic 17, and raw read data or the read data having passed through a decipherment circuit 18 is outputted to the external device in conformity with this judged result.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-314014

(43)公開日 平成5年(1993)11月26日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0 B	9293-5B		
3/06	3 0 4 H	7165-5B		
9/06	4 5 0 A	7232-5B		

審査請求 未請求 請求項の数2(全 5 頁)

(21)出願番号 特願平4-114864

(22)出願日 平成4年(1992)5月7日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 桑原 和義

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

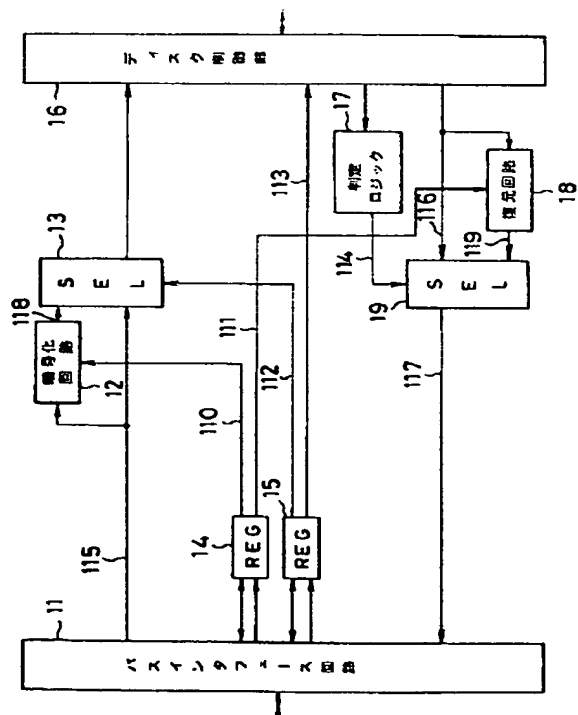
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】 ディスクコントローラ

(57)【要約】

【目的】本発明は、データ暗号化、復元のためのハードウェアをディスクコントローラに内蔵させたことを主な特徴とする。

【構成】外部装置が生成するデータを暗号化して書き込むか否かのデータをレジスタ14に設定し、暗号化キーをレジスタ15に設定して、ディスク装置にデータを書き込む際、それぞれのレジスタ14、15に設定された内容を参照することにより、生の書き込みデータ又は暗号化回路12を経由した書き込みデータを、暗号化したか否かの属性情報とともにディスク制御部16へ出力し、読み込みの際に、読み込みデータが暗号化されているか否かを判定ロジック17によって判断し、その判断結果に従い、生の読み込みデータ又は復元回路18を経由した読み込みデータを外部装置に送出することを特徴とする。



【特許請求の範囲】

【請求項1】 書き込みデータの暗号化指示情報を貯える第1のレジスタ、及び暗号化のためのキー情報を貯える第2のレジスタと、

上記第1のレジスタが暗号化指示状態にあるとき、上記第2のレジスタに貯えられたキー情報を用いて外部より供給された書き込みデータを暗号化処理し、暗号化データであることを示す属性情報を付加してディスクに書き込む手段と、

上記ディスクより読込まれたデータの属性情報をもとに読込みデータが暗号化されているか否かを判断し、読込みデータが暗号化されているとき、上記第2のレジスタに貯えられたキー情報を用いて読込みデータを復号化処理する手段とを具備してなることを特徴とするディスクコントローラ。

【請求項2】 外部より設定される暗号化のためのキー情報を貯える暗号化キーレジスタと、

外部より供給される書き込みデータを暗号化するか否かを示す指示情報を貯えるデータ暗号化レジスタと、

上記暗号化キーレジスタに貯えられたキー情報をもとに外部より供給される書き込みデータに演算を施し書き込みデータを暗号化するデータ暗号化回路と、

上記データ暗号化レジスタが示す指示情報に従い、上記データ暗号化回路を経て出力されるデータ又は外部より供給される生データのいずれか一方を選択し出力する第1のデータセクタと、

この第1のデータセクタを介して出力されるデータに、上記データ暗号化レジスタの内容に従う、書き込みデータが暗号化されているか否かを示す属性情報を付加してディスク上の指定された領域に書き込むデータ書き込み手段と、

上記ディスク上の指定された領域よりデータとそのデータに付随する属性情報を読み込むデータ読込み手段と、上記ディスク上より読込まれた暗号化データを上記暗号化キーレジスタに貯えられたキー情報をもとに復元する復元回路と、

上記ディスク上より読込まれたデータの属性情報をもとに読込みデータが暗号化されているか否かを判定する判定ロジックと、

この判定ロジックの判定結果に従い、上記ディスク上より読込まれた生データ又は上記復元回路を経た読込みデータのいずれか一方を選択し外部へ出力する第2のデータセクタとを具備してなることを特徴とするディスクコントローラ。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 この発明は、特にディスク記憶装置を本体より脱着可能としたパーソナルコンピュータに用いて好適なセキュリティ機能を内蔵したディスクコントローラに関する。

【0002】

【従来の技術】 近年、オフィスでの事務の合理化が進み、その一環として、各自が1台のパーソナルコンピュータをローエンドマシンとして持ち、この各パーソナルコンピュータをLAN回線で共通に接続して、ファイルの共有化を図ったシステムが構築されている。この際、用いられるパーソナルコンピュータは、性能の向上が目覚ましく、デスクトップタイプから、小型、軽量で、携帯に便利な、所謂ラップトップタイプがその主流を占めるようになった。性能的にはデスクトップと同等の遜色もなく、最近では比較的大容量の磁気ディスク装置を補助記憶として標準装備されたものも出現してきている。

【0003】 この種OA（オフィスオートメーション）分野に於いて用いられるパーソナルコンピュータは、現状ではセキュリティ管理がハードウェアもしくはOS（オペレーティングシステム）にて殆どなされていない。その理由は、セキュリティ機能をOSで実現すると、既存OSとの互換性がなくなり、市場に流通している豊富なソフトウェア資産が利用できなくなるという問題が生じることにある。

【0004】

【発明が解決しようとする課題】 上述したように従来のOA分野で使用されるパーソナルコンピュータに於いては、セキュリティ機能をOSで実現すると、既存OSとの互換性がなくなり、市場に流通している豊富なソフトウェア資産が利用できなくなるという問題が生じる。この種パーソナルコンピュータの分野に於いて既存OSとの互換性を維持することが最重要設計事項とされることは周知の通りである。

【0005】 この発明は上記事情に鑑みてなされたもので、データ暗号化／復号化機能をディスクコントローラに持たせることにより、システム本体のCPUに処理負担をかけることなくセキュリティ管理機能を強化したパーソナルコンピュータシステムが容易に構築できるディスクコントローラを提供することを目的とする。

【0006】

【課題を解決するための手段】 本発明のディスクコントローラは、図1に示すように、ディスクへ書き込む書き込みデータを暗号化するか否かの情報を貯えるデータ暗号化レジスタ15と、暗号化のためのキー情報が外部より設定される暗号化キーレジスタ14と、暗号化キーレジスタ14に設定されたキー情報に従い外部装置から供給される書き込みデータに演算を施し暗号化するデータ暗号化回路12と、データ暗号化レジスタ15が示す値に従い、暗号化回路12を経て出力される暗号化された書き込みデータ又は外部装置から供給される生の書き込みデータのいずれか一方を選択する第1のデータセクタ（書き込みデータセクタ）13と、この第1のデータセクタ13で選択されたデータとともに当該データが暗号化さ

れているか否かの属性情報をディスク制御部16へ供給する信号線113と、磁気ディスク装置から読込まれたデータに付随する属性情報に従い当該読込みデータが暗号化されているか否かを判断する判定ロジック17と、磁気ディスク装置より読込まれた暗号化されたデータを上記暗号化キーレジスタ14のキー情報に従い復号化する復元回路18と、磁気ディスク装置より読込まれた生の読込みデータ又は上記復元回路18を経た読込みデータを受けて、上記判定ロジック17の判定結果に従い、いずれか一方のデータを選択する第2のデータセクタ

【0007】

【作用】本発明は、書き込みデータの暗号化処理を選択的に行なうハードウェアと、読込みデータの復元（復号）処理を選択的に行なうハードウェアとをディスクコントローラに持たせて、書き込みデータを任意に暗号化処理してディスクに格納し、復元（復号）処理して外部装置に渡すことができる構成としたもので、これにより、上位の外部装置（例えばパーソナルコンピュータ本体）に処理負担をかけることなく、セキュリティ管理機能の強化が図れる。

【0008】即ち本発明は、ディスクコントローラに、ディスクへ書き込む書き込みデータを暗号化するか否かの情報を貯えるデータ暗号化レジスタと、暗号化のためのキー情報が外部より設定される暗号化キーレジスタとを設け、この各レジスタに、パーソナルコンピュータ本体等の外部装置が生成するデータを暗号化して書き込むか否かのデータと、暗号化のためのキーを設定する。外部より与えられた書き込みデータをディスク装置に書き込む際に、上記各レジスタに設定された内容を参照して、外部より与えられた生の書き込みデータ又は暗号化回路を経たデータをディスク制御部へ出力し、同時に当該データが暗号化されているか否かの情報を属性情報としてディスク制御部へ出力する。ディスク制御部はこの書き込みデータ及び属性情報を磁気ディスクに記録する。ディスク制御部の制御でディスク装置よりデータが読込まれると、判定ロジックがその読込みデータに付随する属性情報から読込みデータが暗号化されているか否かを判定し、その判定結果に従うセクタのデータ選択で、生の読込みデータもしくは復元回路を経由した読込みデータが外部へ送出される。

【0009】これにより、本体CPUに処理負担をかけることなく、磁気ディスク装置の格納データを必要に応じて暗号化でき、セキュリティ管理の強化が図れる。また、暗号化、復元化がOSに依存しないため、既存OSとの互換性が維持され、現在ある豊富なソフトウェア資産を継承することができる。

【0010】

【実施例】以下、図面を使用して本発明の実施例につい

て説明する。図1は本発明の実施例を示すブロック図である。

【0011】図に於いて、符号11はバスインタフェース回路であり、この回路にて本発明の磁気ディスクコントローラと、パーソナルコンピュータ本体等の外部回路とのインタフェース接続がなされる。

【0012】符号12はデータ暗号回路であり、ライン110上の暗号化キーレジスタ14のキー情報に従い、バスインタフェース回路11、及びライン115を介して入力された外部の書き込みデータを暗号化する。

【0013】符号13は書き込みデータセクタ（SEL）であり、ライン112上のデータ暗号化レジスタ15の値により、ライン115を介して供給される生の書き込みデータ、又はライン118上のデータ暗号回路12より出力される書き込みデータのいずれか一方を選択し出力する。

【0014】符号14は暗号化キーレジスタであり、バスインタフェース回路11を介して暗号化／復号化を行なうためのキー情報（キーワード）が設定される。符号15はデータ暗号化レジスタであり、バスインタフェース回路11を介して書き込みデータを暗号化するか否かを示す値が設定される。

【0015】符号16は例えば外部接続される磁気ディスク装置を制御対象下におくディスク制御部であり、外部接続される磁気ディスク装置の機構部を制御するとともに、磁気ディスク装置との間のデータの入出力制御を行なう。ここでは

【0016】符号17はディスクの読込み対象データが暗号化されているか否か（即ち復元（復号化）処理を行なうか否か）を判定する判定ロジックであり、磁気ディスク制御部16からの読込みデータを復元すべきか否かを後述する属性情報に従い決定する。

【0017】符号18はデータ復元回路（データ復号化回路）であり、入力信号ライン116上の読込みデータ（暗号化されたデータ）をライン111上の暗号化キーレジスタ14のキー値をもとに通常の生データに復元する。

【0018】符号19は読込みデータセクタ（SEL）であり、判定ロジック17の判定結果に従い、ライン116上の生の読込みデータ、又はライン119上のデータ復元回路18を経た読込みデータのいずれか一方を選択し、データライン117上に出力する。

【0019】符号110、111は暗号化キー信号ラインであり、暗号化キーレジスタ14の内容を暗号化回路12、及び復元化回路18に伝達する。符号112、113は暗号化セレクト信号ラインであり、データ暗号化レジスタ15に設定された値を書き込みデータセクタ13、及びディスク制御部16に伝達する。符号114は復元化セレクト信号ラインであり、判定ロジック17の判定結果の情報を読込みデータセクタ19に伝達す

5

る。符号115は出力信号ラインであり、バスインタフェース回路11で受けた、CPU、メモリ等の外部回路からの生データを書込みデータセクタ13を介しディスク制御部16に伝達する。符号116は入力信号ラインであり、外部接続される磁気ディスクからのデータを読込みデータセクタ19に伝達する。符号117は復元済み信号ラインであり、このラインを介して読込みデータセクタ19を経たデータがバスインタフェース回路11に転送される。符号118は暗号化回路12の出力を書込みデータセクタ13を介しディスク制御部16に伝達する信号ラインであり、符号119は復元回路18の出力を読込みデータセクタ19、及び復元済み信号ライン117を介しバスインタフェース回路11に伝達する信号ラインである。以下、図1を参照して本発明の実施例の動作について説明する。先ず、ディスク装置への書き込み動作を説明する。

【0020】ディスク装置への書き込みを行なう場合は、書き込みを始めるに際し、磁気ディスクコントローラの外部装置、即ち、図示しないパーソナルコンピュータ本体から、暗号化キーレジスタ14に暗号化キーが書込まれ、データ暗号化レジスタ15に暗号化するか否かの情報が書き込まれる。

【0021】データ書き込みの開始が指示されると、バスインタフェース回路11は、磁気ディスクコントローラの外部装置（パーソナルコンピュータ本体）から供給される書き込みデータを取り込み、ライン115に載せる。ライン115上の信号は、暗号化回路12と書込みデータセクタ13に供給される。

【0022】暗号化回路12は書込みデータセクタ13に設定された値に従って入力データの暗号化を行い、ライン118に載せる。書込みデータセクタ13は、データ暗号化レジスタ12の内容に従い、2つの入力ライン115、118のいずれか一方を選択し、そのライン上のデータをディスク制御部16へ出力する。このとき、データ暗号化レジスタ12の内容は、ライン113によってディスク制御部16へも渡される。

【0023】ディスク制御部16は、書込みデータセクタ13を介して出力される書込みデータに、当該書込みデータが暗号化されているか否かを示すライン113上の属性情報を付随して磁気ディスク装置に書き込む。次に、磁気ディスク装置からのデータの読み込み動作を説明する。

【0024】磁気ディスク装置に格納されたデータの読み込みを行なう場合は、読み込みを始めるに際し、外部装置（パーソナルコンピュータ本体）より、暗号化キーレジスタ14に、暗号化キーを書き込んでおく。

【0025】読み込み開始が指示されると、ディスク制

6

御部16は、磁気ディスク装置から読み込んだデータに付随する属性情報を判定ロジック17に渡し、さらに読込みデータをライン116上に載せる。

【0026】判定ロジック17は、属性情報から、読み込みデータが暗号化データであるか非暗号化データであるかを判定し、その判定結果をライン114を介して読込みデータセクタ19に供給する。ライン116に載せられた読込みデータは、復元回路18、及び読込みデータセクタ19に供給される。

【0027】復元回路18は入力された読込みデータを暗号化キーレジスタ14のキー内容に従い復元（復号処理）し、その復元した読込みデータをライン119上へ出力する。

【0028】読込みデータセクタ19は、ライン114上の判定結果の指示に従い、2つの入力ライン116、119を介して得られる読込みデータのいずれか一方を選択し、ライン117上へ出力する。ライン117上の読込みデータは、バスインタフェース回路11を介して外部装置（パーソナルコンピュータ本体）に内蔵のメモリに転送される。

【0029】尚、上記した実施例では、ディスクコントローラに接続される外部メモリを磁気ディスク装置に限定して説明したが、これに限るものではなく、例えば光ディスク装置、光磁気ディスク装置等にも同様に応用できる。

【0030】

【発明の効果】以上説明のように本発明によれば、ディスクコントローラにデータ暗号化機能を設けた構成としたことにより、磁気ディスク装置をアクセス対象下におく本体CPUに処理負担をかけることなく、セキュリティ管理機能を強化することができる。即ち、従来、本体CPUで行なってきたセキュリティ管理のための暗号化／復号化の処理作業をハードウェア（磁気ディスクコントローラ）で行なうため、本体CPUが持つ本来の性能（処理速度）を十分に活かすことができる。更に、データの圧縮伸張、暗号化、復元化がOSに依存されずハードウェアで実現されるため、現在の豊富なソフトウェア資産を継承することができる。

【図面の簡単な説明】

【図1】本発明の実施例の構成を示すブロック図。

【符号の説明】

11…バスインタフェース回路、12…データ暗号化回路、13…書込みデータセクタ（SEL）、14…暗号化キーレジスタ（REG）、15…データ暗号化レジスタ（REG）、16…ディスク制御部、17…判定ロジック、18…データ復元回路（データ復号化回路）、19…読込みデータセクタ（SEL）。

【図1】

